The Dangers of Getting Picked Up in a Parking Lot

July 2011

ON CYBER PATROL tm
"It's all about the Netv
I ADMIRE ULYSSES FOR INVENTING THE FIRST TROJAN HORSE.
Copyright U.S. Army. All rights reserved.
P.T. BARNUM FOR REALIZING A SUCKER IS BORN EVERY MINUTE.
HURRY! HURRY! HURRY!
THIS WAY TO THE EGRESS
AND GEORGE C. PARKER FOR SELLING THE BROOKLYN BRIDGE A RECORD NUMBER OF TIMES.
DEED
YES, EVEN CYBER CRIMINALS HAVE HEROES.
A1077

You just have to shake your head. According to a recent story in Bloomberg News, the Department of Homeland Security tried a little experiment by dropping CDs and thumb drives in the parking lots of government building and private contractors. Well, one would imagine this would be a great opportunity for our government employees and the specialized contractors that support them to show off their cyber security chops. After all, isn't it a given that these people would have cyber security and information assurance best practices drilled into them? If not, you would at least assume they would have some level of knowledge given the constant flood of cyber security news, alerts and horror stories in the media.

It seems that of those who picked them up, 60 percent plugged the devices into computers in their office. Oh, wait. It gets better. If the drive or CD case had an official logo, our well trained, cyber savvy government employees and contractors plugged in 90 percent of the bogus mobile media. Does that mean that official logos make mobile media that much safer? It would seem so, at least to some.

Now it is possible that in some parts of the country, there are those who would believe that this simply proves that government employees aren't too smart. Pardon the cynicism, but it is likely that the percentages would be the same if the disks and drives were dropped in the parking lots of retail stores, doctor's offices and fast food restaurants. Others might argue that the statistics were easily manipulated, since the quote from the article began with "of those that were picked up." One might argue that it is just as likely that the DHS may have dropped thousands of these test devices, but with only a small fraction actually being picked up. But as we know, it only takes the introduction of one piece of malware onto a network to cause significant damage. So then, do the raw numbers matter? Perhaps not so much.

This isn't picking on certain groups like government employees or patrons of fast food establishments. All this does is highlight why there is a large group of people from all walks of life who are victims of cyber crime.

It also demonstrates why cyber criminals are still using phishing techniques like get rich quick schemes, opportunities for adult encounters and pleas for help from rich but oppressed citizens of foreign countries. It shows why cyber "baddies" still hang around in internet cafes or drive around suburban neighborhoods gleaning private data from ill protected networks. It shows why dedicated hackers can breach the online security of the Sony Corporation, the Central Intelligence Agency and various other U.S. government web sites for no other reason than simply because they can.

There are few who engage in a struggle against an opposing force that are not familiar with the insight and wisdom of the ancient Chinese General Sun Tsu. Indeed, everyone from computer war gamers to four star generals are often heard to quote him. His advice on waging war is as applicable in corporate board rooms as it is in Command and Control Centers. Of all the general's famous quotes, there is one that those who protect data should find chilling , especially coming from a cyber criminal or foreign agent; "Can you imagine what I would do if I could do all I can?"